IN THE CLAIMS:

Claims 1-20 (canceled)

Please enter new claims 21-32 as follows:

21. (New) A method of detecting intrusions, said method comprising the steps of:

storing a plurality of intrusion signatures;

automatically detecting a multiplicity of system events having respective signatures;

comparing each of said multiplicity of system event signatures to said plurality of intrusion signatures;

recording a number of times that each of said intrusion signatures matched said system event signatures;

automatically ordering the stored plurality of intrusion signatures based on how many times each of said intrusion signatures matched said system event signatures, such that the intrusion signature matching the most system event signatures is first in the order; and

subsequently comparing a signature of a subsequent system event with said plurality of intrusion signatures in said order.

22. (New) A method as set forth in claim 21 further comprising the step of:

sending alerts in response to matches of said system event signatures to said intrusion signatures.

23. (New) A method as set forth in claim 21 wherein each intrusion signature is associated with a respective action to perform in response to a predetermined number of said system event signatures matching said each intrusion signature.

24. (New) A system for detecting intrusions, said system comprising:

a table storing a plurality of intrusion signatures;

means for detecting a multiplicity of system events having respective signatures;

means for comparing each of said multiplicity of system event signatures to said plurality of intrusion signatures;

means for recording a number of times that each of said intrusion signatures matches said system event signatures;

means for ordering the stored plurality of intrusion signatures based on how many times each of said intrusion signatures matches said system event signatures, such that the intrusion signature matching the most system event signatures is first in the order; and

means for subsequently comparing a signature of a subsequent system event with said plurality of intrusion signatures in said order.

25. (New) A system as set forth in claim 24 further comprising:

means for sending alerts in response to matches of said system event signatures to said intrusion signatures.

26. (New) A system as set forth in claim 24 wherein each intrusion signature is associated with a respective action to perform in response to a predetermined number of said system event signatures matching said each intrusion signature.

27. (New) A method of detecting intrusions, said method comprising the steps of:

storing a plurality of intrusion signatures and identifications of respective actions to perform when a predetermined number of system event signatures match the respective intrusion signature;

automatically detecting a subsequent system event having a signature;

comparing the subsequent system event signature with said plurality of intrusion signatures, and if no match is found, storing said subsequent system event signature in association with said plurality of intrusion signatures and also storing an indication that no corrective action is needed in response to detection of said subsequent system event;

later, automatically detecting a plurality of other system events having respective signatures; and

comparing the other system event signatures to said plurality of intrusion signatures and said subsequent system event signature, and performing the actions, if any, indicated by matches of said other system event signatures to said plurality of intrusion signatures and said subsequent system event signature.

28. (New) A method as set forth in claim 27 further comprising the steps of:

recording a number of times that each of said plurality of intrusion signatures matches said other system event signatures, and recording a number of times that said subsequent system event signature matches said other system event signature; and

ordering the stored plurality of intrusion signatures and said subsequent system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said subsequent system event signature, such that the signature for which the most number of times has been recorded is first in the order.

29. (New) A system for detecting intrusions, said system comprising:

a table storing a plurality of intrusion signatures and identifications of respective actions to perform when a predetermined number of system event signatures match the respective intrusion signature;

means for detecting a subsequent system event having a signature;

means for comparing the subsequent system event signature with said plurality of intrusion signatures, and if no match is found, storing said subsequent system event signature in association with said plurality of intrusion signatures and also storing an indication that no corrective action is needed in response to detection of said subsequent system event;

means for automatically detecting a plurality of other, later system events having respective signatures; and

means for comparing the other system event signatures to said plurality of intrusion signatures and said subsequent system event signature, and performing the actions, if any, indicated by matches of said other system event signatures to said plurality of intrusion signatures and said subsequent system event signature.

30. (New) A system as set forth in claim 29 further comprising:

means for recording a number of times that each of said plurality of intrusion signatures matches said other system event signatures, and recording a number of times that said subsequent system event signature matches said other system event signature; and

means for ordering the stored plurality of intrusion signatures and said subsequent system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said subsequent system event signature, such that the signature for which the most number of times has been recorded is first in the order.

31. (New) A method of detecting intrusions, said method comprising the steps of:

storing a plurality of intrusion signatures;

automatically detecting a multiplicity of system events having respective signatures;

comparing each of the multiplicity of system event signatures to said plurality of intrusion signatures, one of said system event signatures not matching any of said intrusion signatures and not corresponding to an intrusion, and other of said system event signatures matching respective ones of said intrusion signatures; and

storing said one system event signature in association with said plurality of intrusion signatures;

recording a number of times that said each of said intrusion signatures matches a respective one of said system event signatures;

recording a number of times that said one system event has occurred;

subsequently ordering the stored plurality of intrusion signatures and said one system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said one system event signature, such that the signature for which the most number of times has been recorded is first in the order; and

subsequently comparing a signature of a subsequent system event with said signatures in said order until finding a match between said subsequent system event signature and one of said signatures in said order.

32. (New) A system for detecting intrusions, said system comprising:

a table storing a plurality of intrusion signatures;

means for detecting a multiplicity of system events having respective signatures;

means for comparing each of the multiplicity of system event signatures to said plurality of intrusion signatures, one of said system event signatures not matching any of said intrusion signatures and not corresponding to an intrusion, and other of said system event signatures matching respective ones of said intrusion signatures;

means for storing said one system event signature in association with said plurality of intrusion signatures;

means for recording a number of times that each of said intrusion signatures matches a respective one of said system event signatures;

means for recording a number of times that said one system event has occurred;

means for subsequently ordering the stored plurality of intrusion signatures and said one system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said one system event signature, such that the signature for which the most number of times has been recorded is first in the order; and

means for subsequently comparing a signature of a subsequent system event with said signatures in said order until finding a match between said subsequent system event signature and one of said signatures in said order.